AUTONOMOUS DECISION-MAKING IN ARMED CONFLICT. EVALUATING THE LAWS OF WAR THROUGH THE GAZA EXPERIENCE

Adeshina SOWEMIMO[1]
https://doi.org/10.54989/stusec.2026.20.01.02

Abstract

Autonomous targeting systems are becoming more common and established as an armament system, yet international humanitarian law (IHL) was designed for human decision-makers, not algorithms. Focusing on the 2023-24 Gaza conflict, this study questions the effectiveness of existing legal frameworks applied during a conflict in which reports indicate AI systems, such as Lavender, Habsora, and Where's Daddy?, were used to generate targets at unprecedented levels and speeds in modern warfare.

Based on Critical Algorithm Studies and socio-technical assemblage theory, and using a legal-analytical, case-based approach, the study investigates the meaning and implications of IHL principles of distinction, proportionality, and precaution in an algorithmic context, and their failure. It found that the existing frameworks are structurally deficient because the operational conditions of AI-assisted targeting systematically undermine the cognitive and institutional practices that underpin compliance.

This phenomenon, digital dehumanization, in which people are treated as part of a probabilistic data classification rather than as legal persons - widens compliance gaps and, in certain cases, leads to new legal breaches. The study concludes with concrete governance proposals, such as auditability standards, disaggregated liability-attribution frameworks, and minimum human-verification protocols, as the basis for an AI-specific legal regime suitable to contemporary algorithmic warfare.

Keywords: AI-assisted targeting; Digital dehumanization; International Humanitarian Law (IHL); Lethal Autonomous Weapon Systems (LAWS)

Introduction

Autonomous Weapon Systems (AWS) are gravitating from speculative technology to active tools in contemporary battlefields. This trend raises concern among actors because the law governing armed conflict is still heavily hinged on subtle assumptions about human judgment and responsibility. International Humanitarian Law (IHL) aims to strike a delicate balance between military necessity and the principles of humanity. Yet it does so with human decision-makers in mind, not machines that may select or engage targets on their own.[2,3] Within the context of weapons systems, the concept of autonomy is layered. There is the human perspective, which concerns itself with the level of control humans exert over

[1] Adeshina Sowemimo is a Lecturer in the Department of Political Science, University of Benin, Benin City, Nigeria. His research interests include comparative politics and international relations; https:orcid.org/0009-0009-6838-4737; adeshina.sowemimo@uniben.edu.

[2] Diakonia, *Basic Principles of International Humanitarian Law*, Diakonia, https://www.diakonia.se/ihl/resources/international-humanitarian-law/basic-principles-ihl/ (12.11.2025)

[3] Anaïs Maroonian, "Proportionality in International Humanitarian Law: A Principle and a Rule," Lieber Institute for Law and Warfare, October 2022, https://lieber.westpoint.edu/proportionality-international-humanitarian-law-principle-rule/ (12.11.2025)

machines. Here, humans could be in, on or out of the loop[1]. While in the loop, humans select and engage targets through the machine's agency. While on the loop, the machine selects and engages the target, while humans retain oversight and the option to override the machine's decisions manually. Humans are out of the loop when the machines select and engage the target without requiring any human input beyond activation.

The second perspective concerns itself with the level of complexity and intelligence of the machine. From this perspective, the machine could be automatic, automated or autonomous. The machine is automatic to the extent that it has simple mechanical responses to environmental input. It is automated through a complex but predictable algorithm that operates on if-then-else logic. A machine that self-directs upon activation and possesses the capacity for self-learning and upgrading, to the extent of acting beyond the limits of its initial codes in a fully autonomous system.[2] The third perspective on defining autonomy is not much about autonomy itself but the nature of the task assigned to the machine. The critical function that defines autonomy is the selection and engagement with targets.[3] This is where autonomy directly intersects with the fundamental principles of IHL.[4] This complexity shapes the ongoing struggle to define what should count as an Autonomous Weapon System. States working within the United Nations (UN) Convention on Certain Conventional Weapons (CCW) process, along with scholars and advocacy groups, hold sharply different views.

The broad perspective, most prominently advanced by the International Committee of the Red Cross (ICRC), defines AWS as any weapon system that can select and attack targets without human intervention in its critical functions, namely, the processes of identifying, selecting, and applying force against a target.[5] This framing includes both fully autonomous and semi-autonomous systems, provided that autonomy is exercised in one or more of these decisive stages. On the other hand, for the United States (US) Department of Defense (DoD), AWS are systems that "once activated, can select and engage targets without further intervention by a human operator"[6]. This narrow perspective excludes decision-support systems, AI-assisted targeting software, or predictive analytical tools similar to those reportedly used in Gaza in the period under review. The United Nations Group of Governmental Experts (GGE) under the Convention on Certain Conventional Weapons (CCW) highlighted this definitional tension in its reports from 2019 to 2024.[7] States like Austria and many from the Global South have aligned with the broader framing, highlighting the continuum of autonomy and the dangers of algorithmic decision-making even in non-lethal dimensions. Other countries, including the United States, Israel, and Russia, have favored the narrower definition, limiting AWS to fully autonomous systems. This definition

---

Maziar Homayounnejad, *Regulating Lethal Autonomous Weapon Systems I: Assessing the Sense and Scope of 'Autonomy'*, "Emerging Military Weapon Systems", TLI Think Paper 76, The Dickson Poon School of Law, King's College London, 2017, https://ssrn.com/abstract=3027540 (12.11.2025)

[2] Maziar Homayounnejad, *Op. cit,* p. 10

[3] *Ibidem*, p. 11

[4] Neil Davison, *What You Need to Know about Autonomous Weapons*, International Committee of the Red Cross (ICRC), https://www.icrc.org/en/document/what-you-need-know-about-autonomous-weapons (12.11.2025)

[5] International Committee of the Red Cross (ICRC), *Autonomous Weapon Systems: Implications of Increasing Autonomy in the Critical Functions of Weapons*, ICRC, Geneva, 2016, pp. 5-6

[6] U.S. Department of Defense, *Directive 3000.09: Autonomy in Weapon Systems*, DoD, Washington, D.C., Updated 2023, Sec. 3(a)

[7] United Nations, *Report of the 2019 Session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems*, CCW/GGE.1/2019/3, United Nations Office, Geneva, 2019

divide is also prominent in scholarly discourse. Sharkey and Roff construe AWS as a spectrum of autonomy, ranging from lethal to non-lethal systems.[1] For Arkin, AWS is a system that is completely independent upon activation.[2] This study aligns with the ICRC's broad definitional approach, which provides a more accurate analytical framework for evaluating AWS deployment in Gaza and its compliance with the principles of distinction, proportionality, and precaution under International Humanitarian Law.

Beneath the definitional trouble lies a deeper question: can autonomy be squared with the core principles of IHL? Proponents argue that AWS could enhance compliance with International Humanitarian Law (IHL) by reducing human error, improving precision, and limiting emotional or retaliatory impulses in combat.[3] Arkin is of the view that autonomous systems can be engineered to comply with the laws of war more effectively than human soldiers, who are susceptible to fatigue, fear, and bias.[4] Anderson and Waxman opine that a ban on AWS would be hasty and amount to stifling technological progress, highlighting that the existing legal framework of IHL sufficiently governs the responsible development and deployment of AWS.[5] These arguments often rest on the assumption that autonomy, when properly engineered, can lead to more discriminating and proportional deployment of force. Critics, however, counter that AWS risks eroding the moral agency and accountability that underpin humanitarian law.[6] Sharkey argues that delegating life-and-death decisions to machines negates the principle of human judgment central to jus in bello.[7] The International Committee of the Red Cross (ICRC) and similar organizations warn that the opaqueness of machine-learning algorithms and the fluidity of complex combat environments make it impractical to ensure reliable compliance with the principles of distinction, proportionality, and precaution.[8] Heather Roff stresses that even semi-autonomous systems introduce new layers of uncertainty and bias into targeting processes.[9] From this standpoint, AWS poses technical challenges on the one hand and, on the other, a normative concern that could blur human accountability in combat, eroding the moral limits that IHL was designed to preserve.

Purpose and Objectives

Current research in the field of AWS reflects a lack of conceptual cohesion, with technical debates intersecting with legal uncertainties, and ethical concerns blurring into policy challenges. This complexity is the central problematic that informs the present study. The ongoing advancement and practical deployment of Artificial Intelligence (AI) and Machine Learning (ML) technologies in contemporary warfare stand in stark contrast to the absence of a robust shared framework for their understanding and governance. The above reality makes it difficult to measure the actual (or potential) compliance of AWS with the core

[1] Noel Sharkey, *Killing Made Easy: From Joysticks to Politics*, in Patrick Lin; Keith Abney; George A. Bekey (Eds.), "Robot Ethics: The Ethical and Social Implications of Robotics", MIT Press, Cambridge (MA), 2012, pp. 111-128
[2] Ronald C. Arkin, *Governing Lethal Behavior in Autonomous Robots*, CRC Press, Boca Raton, 2009
[3] Ronald Arkin, *Op, cit.,* p. 39
[4] *Idem*
[5] Kenneth Anderson, Matthew Waxman, *Op, cit.,* p. 8
[6] Human Rights Watch, *Losing Humanity: The Case Against Killer Robots*, HRW, New York, 2012, pp. 2-5.
[7] Noel Sharkey, *The Evitability of Autonomous Robot Warfar*e, "International Review of the Red Cross", Vol. 94, No. 886, 2012, pp. 787-799
[8] International Committee of the Red Cross (ICRC), *Autonomous Weapon Systems: Implications of Increasing Autonomy in the Critical Functions of Weapons*, ICRC, Geneva, 2016, pp. 5-8
[9] Heather M. Roff, Op. cit., p. 218; *The Strategic Robot Problem: Lethal Autonomous Weapons in War*, "Journal of Military Ethics", Vol. 13, No. 3, 2014, pp. 211-227

principles of international humanitarian law (IHL). A case-by-case evaluation is endorsed as an effective approach to assessing AWS's compliance with IHL.

As Winter observes, "assessments must be made on a case-by-case basis, with reference to the specific parameters of each autonomous weapon system and the environment in which it will operate" since compliance depends on technological capability and context. Schmitt shares Winter's position, noting that mere possession of AWS does not, in itself, constitute sufficient grounds for a violation under IHL, but its unlawful deployment does[1] [2]. These perspectives underscore that responsible deployment of AWS requires individualized, multidisciplinary review rather than categorical judgments. Rather than seeking a sweeping, universal answer about all of AWS, this study will examine specific systems, their practical deployments, their technical feasibility, the operational environments in which they were deployed, and the nature of their assigned tasks. This will be done from a practical standpoint, determining their compliance with the principles of distinction, proportionality, and precaution, which are cornerstones of the IHL framework.

Some studies have adopted this case-by-case approach to the AWS debate, including in the Gaza theatre. Some scholars have adopted the case-study methodology to interrogate how autonomy functions in real combat environments. The United States' use of the Aegis Combat System and the Patriot missile defense system in incidents such as the USS *Vincennes* shootdown, 1988, and the 2003 Iraq War have long been treated as early empirical sites for examining "automated lethality"[3]. Arkin and Anderson argue that partial autonomy has existed for decades and that case-specific reviews provide practical pathways to appraising compliance with IHL principles.[4] Similarly, Roff's study on the Harpy loitering munition shows that even limited autonomy in deployment creates operational uncertainties in complex environments.[5] The United Nations Institute for Disarmament Research (UNIDIR) has compiled comparative case studies on emerging AWS, highlighting the fluidity of autonomy and its opacity to external verification.[6] More recently, investigative journalism and policy-oriented studies on Israel's 2023-24 campaign in Gaza have documented the deployment of AI-driven systems for labelling terrorists, target generation, and real-time tracking, representing the most current empirical attempt to test theoretical claims about AWS precision and control[7].

However, these works do not offer a highly granular, publicly verified study of offensive AWS use in a dense urban environment such as Gaza between 2023-24, with named systems and strike-by-strike analysis. The recent Gaza-focused investigations, though groundbreaking, operate in the grey zone between journalistic exposé and formal academic inquiry, leaving many technical details unverifiable.[8] The overall objective is to empirically

[1] Elliot Winter, *The Compatibility of Autonomous Weapons with the Principles of International Humanitarian Law*, "Journal of Conflict and Security Law", Vol. 27, No. 1, 2022, pp. 6-7
[2] Michael N. Schmitt, *Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics*, "Harvard National Security Journal Feature", 2013, p. 25
[3] Paul Scharre, *Army of None: Autonomous Weapons and the Future of War*, W. W. Norton, New York, 2018, pp. 62-70
[4] Ronald C. Arkin, *Op. cit*., p. 93
[5] Heather M. Roff, *Op. cit.*, p. 218
[6] United Nations Institute for Disarmament Research (UNIDIR), *The Weaponization of Increasingly Autonomous Technologies: Autonomous Weapon Systems and Cyber Operations*, UNIDIR, Geneva, 2017, pp. 14-18
[7] Yuval Abraham, *Lavender: The AI Machine Identifying Targets in Israel's Gaza War*, "+972 Magazine", April 2024
[8] *Idem*

evaluate the compliance of those AWS deployments (or alleged deployments) with the IHL principles of distinction, proportionality, and precaution in attack.

Critical Algorithm and Socio-Technical Assemblage

The study builds its theoretical underpinning on two frameworks to systematically interrogate the Gaza operations of 2023–2024 from the perspectives of compliance with core IHL principles and the impact of the use of autonomous and semi-autonomous targeting tools. The Critical Algorithm Studies (CAS) are an interdisciplinary space whose focus is to analyses the inner workings of the systems referenced, in relation to the algorithm being created and the institutional values that guide it. This was complemented by the Socio-Technical Assemblage theory, which helps understand that technologies are not simply devices but are interwoven in a network of people, institutions, and material infrastructures that shape AWS performance. The Critical Algorithm lens draws on work by scholars such as Gillespie, Crawford, Kalluri, and others who argue that algorithms reflect the politics of their datasets, the incentives of the institutions that deploy them, and the shortcuts embedded in their design choices.[1] This matters for Gaza because the systems at the center of the debate (and related target-development pipelines) did not operate in a vacuum. Their strike suggestions were based on training data of varying quality, behavioral proxies selected by analysts, and thresholds set during periods of operational pressure[2].

The second lens builds on the work of scholars such as Latour, Suchman, Crampton, and Chamayou. It treats AWS not as isolated devices but as nodes inside a wider network of command structures, targeting cells, lawyers, data engineers, pilots, and communication channels. A strike attributed to an autonomous system is therefore better understood as the outcome of interactions across the whole assemblage.[3] This framework prompts a careful mapping of how information moved through the kill chain during the Gaza operations, drawing attention to distributed agency and the material infrastructures through which decisions were enacted[4]. It also sets up the study to examine where human judgment entered the loop and where it thinned out[5]. This approach supports the study's objective by focusing on how organizational routines either tightened or weakened IHL-relevant safeguards. It also helps explain the gap between stated doctrine and observed strike patterns[6].

Critical Algorithm Studies aids analysis by identifying what each system was crafted to accomplish, its functional reliability, and the built-in error margins in the Gaza context. This feeds into the assessment of whether the systems could realistically support distinction, proportionality, and precaution. The socio-technical assemblage paradigm prompts the examination of how the urban environment, communication constraints, sensor coverage, and battle damage assessments shaped system outputs. It supports the proportionality analysis by showing how these constraints interact with algorithm-assisted targeting. Integrating both frameworks enables the study to track how algorithm-aided target recommendations, real-time

[1] Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*, Yale University Press, New Haven, 2018, pp. 12-18, 45–52; Pratyusha Kalluri, *Don't Ask If Artificial Intelligence Is Good or Fair, Ask How It Shifts Power*, "Nature", No. 583, 2020, p. 169
[2] Yuval Abraham, *Op. cit.*, p. 2
[3] Bruno Latour, *Reassembling the Social: An Introduction to Actor-Network-Theory*, Oxford University Press, Oxford, 2005
[4] Lucy Suchman, *Human-Machine Reconfigurations: Plans and Situated Actions*, 2nd Ed., Cambridge University Press, Cambridge, 2007
[5] Mark B. Salter, Jeremy W. Crampton, *Introduction: Field Guide to Security Assemblages, in Security/Geography: A Field Guide to Security Assemblages*, University of Georgia Press, Athens, 2014
[6] Grégoire Chamayou, *A Theory of the Drone*, trans. Janet Lloyd, The New Press, New York, 2015

tracking flowed through human decision-making and ultimately contributed to the actual strikes, permitting a direct evaluation of whether the structural design of the assemblage made lawful outcomes more or less likely. Put together, the two frameworks link the conceptual debate on AWS to a practical evaluation of the systems deployed in Gaza. It grounds the popular legal analysis in the realities of how these systems operate, why certain strike patterns emerged, and where compliance gaps may reside.

AI-Assisted Targeting Systems and the Transformation of the Targeting Cycle in Gaza

Investigative reporting and scholarly engagement have highlighted the IDF's deployment of specific algorithm-assisted systems, including "The Gospel" (or Habsora, in Hebrew), "Lavender", and a real-time tracking tool named "Where's Daddy" in the military operations conducted by the IDF in the Gaza Strip between 2023 and 2024, codenamed Swords of Iron. Though their system card remains classified, available accounts suggest that they constitute part of a layered intelligence infrastructure designed to process large volumes of surveillance and intelligence data and generate potential recommendations.[1] This level of adoption reflects the broader increasing reliance on artificial intelligence and machine-learning tools in contemporary warfare.[2] At the design level, these systems perform distinct but related functions across the phases of the targeting cycle. Lavender is a machine-learning tool designed to identify suspected militants by analyzing communications metadata, digital behavioral traces, and historical intelligence records. These inputs can include belonging to the same WhatsApp group with a known militant, frequently changing one's phone and address, cellular information, social media connections, battlefield information, phone contacts, and pictures in phone galleries.[3] Investigative reporting indicates that in the opening weeks of the war, Lavender flagged about 37,000 individuals as militants, and that these recommendations were accorded the integrity of human outputs. This volume suggests a target identification scale that dwarfs the capacity of traditional human-dominated intelligence processes.[4] This is indicative of a broader shift toward high-volume, data-driven target generation.

In contrast, Habsora operates at the level of infrastructure analysis, processing geospatial intelligence and other data to identify buildings or locations believed to be associated with militant activity. Similar to Lavender, it processes enormous amounts of data that rival the capacity of thousands of intelligence officers while producing real-time bombing-site recommendations[5]. The third system under review, "Where's Daddy?", operates downstream from these identification processes by monitoring the movement patterns of individuals previously flagged as militants and notifying operators when they arrive at particular strike-suitable locations, mostly their homes.[6] Collectively, these systems suggest an architecture in which algorithmic tools operate sequentially across the targeting cycle, identifying suspected militants, identifying structures associated with militant activities, and

[1] Yuval Abraham, *Op. cit.*, p. 2
[2] Paul Scharre, *Army of None: Autonomous Weapons and the Future of War*, W. W. Norton, New York, 2018, p. 8-9, p. 65, pp. 346-347; Michael C. Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics*, Princeton University Press, Princeton, 2010, p. 4-5, 217
[3] Yuval Abraham, *Op. cit.*, p. 2
[4] *Idem*
[5] Yuval Abraham, *A Mass Assassination Factory: Inside Israel's Calculated Bombing of Gaza*, "+972 Magazine", 2023, https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza/ (12.02.2026)
[6] *Idem*

monitoring the movements of previously flagged individuals until they arrive at suitable potential strike locations.

These systems rely on extensive data infrastructures capable of processing diverse forms of intelligence generated through signals interception, satellite imagery, telecommunications metadata, and other forms of digital monitoring. Machine-learning models are particularly suited to analysing these datasets because they can detect statistical patterns across large volumes of data that may be difficult for human analysts to identify. They are valued for their ability to transform complex data streams into structured analytical outputs that guide human attention toward potentially relevant signals[1].

Among other factors, the reliability of algorithmic analysis significantly depends on the quality and structure of its data environment. The outputs of Machine Learning systems are a product of input datasets that may be incomplete, unclear, or poorly validated, particularly when data is voluminous and varies in reliability.[2] When data sets are plagued with gaps and outdated information, they introduce and propagate systematic bias into models, complicating analysis, reducing predictive validity, and producing unreliable outcomes.[3] In densely populated urban environments such as Gaza, where civilian populations and militants share communications infrastructure and residential spaces, behavioral data can become difficult to interpret reliably. Research on algorithmic decision-making submits that biases and errors in training datasets propagate through automated classification systems and become amplified when algorithms operate at scale.[4] These dynamic raises concern that flawed data may influence algorithmic classifications in ways that are difficult for human reviewers to detect. Reports on the referenced conflict submitted that some data used to inform the recommendations of the AI-assisted targeting systems deployed was flawed, and that human operators failed to detect the attendant errors in those recommendations. Lavender had an estimated margin of error that human reviewers accepted under operational urgency.[5] Human Rights Watch corroborated the claim, submitting that AI-assisted targeting tools were fed defective data and inaccurate approximations, including bogus geolocation and metadata proxies.[6] In such circumstances, recommendations were derived from probabilistic pattern matching across defective datasets, making it difficult for human reviewers to objectively assess their reliability, particularly under conditions of high operational tempo[7].

The organizational workflow through which algorithmic outputs are integrated into military decision-making structures is also of significant importance. AI-assisted targeting

[1] Kate Crawford, *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*, Yale University Press, New Haven, 2021

[2] International Committee of the Red Cross (2019/2023); Paulus et al., 2019; GCHQ cited in AI intelligence literature.

[3] Solon Barocas, Moritz Hardt, Arvind Narayanan, *Fairness and Machine Learning*, 2023; Cathy O'Neil, *Weapons of Math Destruction*, Crown, New York, 2016; K. Emmanuel et al., *A Survey on Missing Data in Machine Learning*, "Journal of Big Data 8", No. 1, 2021, p. 140

[4] Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* Crown, New York, 2016

[5] Yuval Abraham, *Op. cit.*, p. 2

[6] Human Rights Watch, *Questions and Answers: Israeli Military's Use of Digital Tools in Gaza*, 2024, https://www.hrw.org/news/2024/09/10/questions-and-answers-israeli-militarys-use-digital-tools-gaza (21.02.2026)

[7] Lisa Wiese, Charlotte Langer, *Gaza, Artificial Intelligence, and Kill Lists*, "Verfassungsblog", May 16, 2024, https://verfassungsblog.de/gaza-artificial-intelligence-and-kill-lists/, DOI: 10.59704/07a0756a3c08e64a; Royal United Services Institute, *The Israel Defense Forces' Use of AI in Gaza: A Case of Misplaced Purpose*?, 2024, https://www.rusi.org/explore-our-research/publications/commentary/israel-defense-forces-use-ai-gaza-case-misplaced-purpose (21.02.2026)

systems ideally function as decision-support tools rather than autonomous weapons, meaning that their outputs are reviewed by human analysts before operational decisions are taken. Within military institutions, this process typically involves intelligence analysts who interpret algorithmic recommendations, operational planners who evaluate potential strike options, and legal advisers who assess compliance with IHL[1]. In principle, this structure ensures that responsibility for the use of force resides with human decision-makers. However, the adoption of AI-enabled target recommendation systems can reshape how analysts interact with intelligence information. When algorithms generate large numbers of potential targets in short periods, analysts may increasingly over-rely on these outputs to cope with information overload, even when independent verification might be warranted. Research in human-machine interaction captures this dynamic as automation bias.[2] Empirical accounts indicate that the IDF dealt with the AI-systems-induced recommendation overload through a combination of temporal compression, cognitive delegation, and organizational adaptation[3]. There were documented instances in which the duration of human review of AI-system-generated recommendations lasted only 20 seconds, with reviewers' roles sometimes limited to gender confirmation.[4] Rather than treating errors as anomalies to be resolved, operators accepted varying margins of error in algorithmic classifications, thereby tacitly institutionalizing uncertainty in high-tempo operations.[5] Analysts had their roles reduced to filtering AI-generated recommendations rather than independent target identification. [6] Overall, the scaling effects of these systems contributed to what has been aptly described as a "target factory" model, with the rate of target generation dramatically outnumbering that of previous Gaza conflicts[7].

These institutional dynamics hold implications concerning the legal and ethical framework governing armed conflict. International humanitarian law requires that parties to a conflict distinguish between combatants and non-combatants, ensure that anticipated civilian harm is not excessive compared to anticipated military advantage, and take all feasible precautions in the use of force.[8] A Human Rights Watch investigation into an Israeli airstrike on a residential building in central Gaza revealed that the attack killed at least 106 civilians without a definite military objective, leading the organization to classify it a war crime[9]. Amnesty International documented repeated strikes on residential buildings in Gaza that resulted in the deaths of entire households, often in circumstances where the presence of a

[1] Paul Scharre, *Op. cit.*, p. 55, p. 98, p. 129, p. 191, p. 216; Kate Crawford, *Op. cit.*, p. 189
[2] Raja Parasuraman and Victor Riley, *Humans and Automation: Use, Misuse, Disuse, Abuse*, "Human Factors", Vol. 39, No. 2, 1997, pp. 230–253, https://doi.org/10.1518/001872097778543886
[3] Royal United Services Institute, *The Israel Defense Forces' Use of AI in Gaza: A Case of Misplaced Purpose?*, 2024
[4] Business Insider, *Israel's Use of AI in Gaza Offers a Glimpse into the Future of Warfare*", April 2024; Yuval Abraham, *Op. cit.,* p. 3
[5] Le Monde, *Israeli Army Uses AI to Identify Tens of Thousands of Targets in Gaza*, April 5, 2024; Abraham, *Op. cit.*, p. 34
[6] Yuval Abraham, *A Mass Assassination Factory: Inside Israel's Calculated Bombing of Gaza*, "+972 Magazine", 2023; The Guardian, *The Gospel: How Israel Uses AI to Select Bombing Targets in Gaza*, December 1, 2023
[7] *Idem*
[8] International Committee of the Red Cross, *Customary International Humanitarian Law, Volume I: Rules*, Cambridge University Press, Cambridge, 2005
[9] Human Rights Watch, *Gaza: Israeli Strike Killing 106 Civilians an Apparent War Crime*, April 4, 2024, https://www.hrw.org/news/2024/04/04/gaza-israeli-strike-killing-106-civilians-an-apparent-war-crime (12.03.2026)

target and by implication the existence of a significant military objective was unclear.[1] A broader assessment by Human Rights Watch submitted that several Israeli attacks during the referenced campaign resulted in high civilian casualties relative to the anticipated military advantage, raising concerns about disproportionate use of force.[2] This question is whether meaningful attention was paid to proportionality assessments or whether they were ignored under military exigencies triggered by a surge in recommendations from AI-assisted systems.

Beyond operational concerns, the deployment of AI-assisted targeting systems also holds broader strategic and political implications. Added to signaling technological sophistication in the international security environment, armed conflicts also constitute environments in which emerging technologies are tested and refined under operational conditions.[3] The reported IDF deployment of algorithmic targeting systems in Gaza, along with the observed impact on the tempo of warfare, may have been an opportunity for the IDF to signal military sophistication while testing and refining AI-enabled targeting systems under real combat conditions. The initial volume of AI-systems recommendations in the first few weeks and the eventual tapering as the conflict progressed may suggest testing and refinement.

The increasing adoption of algorithmic targeting systems in contemporary warfare and their multiplier effect on the tempo of armed conflict (as observed in Gaza) may indicate a deeper shift in how militaries define potential targets. When algorithmic systems translate complex social realities into statistical indicators of suspected affiliation, humans may be represented primarily as probabilistic classifications rather than as real people embedded within a broader civilian environment.[4] As combatants and non-combatants in conflict environments increasingly appear as data profiles (constructed from behavioral signals, communication patterns, or network associations) within military information systems, warfare may gradually lose touch with humanity. This disturbing dynamic is aptly captured as "digital dehumanization". With reference to the referenced Gaza conflict, digital dehumanization does not necessarily arise from a conscious disregard for human life. It is more likely an inadvertent product of the operational logic of Algorithmic systems that process complex social identities and relationships into computational categories for rapid processing. In a densely populated environment like Gaza, with civilians and militants sharing infrastructure and communications networks, algorithmic classifications that over-rely on relational or behavioral indicators may risk blurring legally and morally significant distinctions.[5] The trade-off for attaining enhanced analytical efficiency in this context is an obscured social context in which behaviors occur. The increasing adoption of AI in military intelligence assemblages can influence decision-making patterns by prioritizing machine-generated recommendations, which can, on the one hand, reshape the definition of potential targets and, on the other, subtly redefine the acceptable threshold of risk in the use of force[6].

---

[1] Amnesty International, *Damning Evidence of War Crimes as Israeli Attacks Wipe Out Entire Families in Gaza*, October 20, 2023, https://www.amnesty.org/en/latest/news/2023/10/damning-evidence-of-war-crimes-as-israeli-attacks-wipe-out-entire-families-in-gaza/ (12.03.2026)

[2] Human Rights Watch, *Gaza: Israeli Strike Killing 106 Civilians an Apparent War Crime*, April 4, 2024, https://www.hrw.org/news/2024/04/04/gaza-israeli-strike-killing-106-civilians-an-apparent-war-crime (12.03.2026)

[3] Michael C. Horowitz, *Op. cit.*, p. 43

[4] Kate Crawford, *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*, Yale University Press, New Haven, 2021

[5] Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Crown Publishing, 2016

[6] Paul Scharre, *Op. cit.*, p. 98, p. 168; Kate Crawford, *Op. cit.*, p. 203

Reports indicate that the IDF adopted scaled collateral damage thresholds, allowing between 15 and 20 civilian casualties for a strike on senior Hamas commanders and lower thresholds, sometimes reaching 10, for lower-ranking operatives, while also pragmatically delegating strike authorizations, previously the preserve of senior officers, to mid-level officers[1].

The ICRC and UN-based forums, like the CCW Group of Governmental Experts on Lethal Autonomous Weapons Systems, have highlighted that meaningful human control be maintained over decisions regarding the use of force, reflecting a growing consensus that human agency cannot be eliminated in life-and-death targeting processes[2]. In a similar vein, emerging scholarship emphasizes that, to preserve accountability and protect non-combatants in conflict zones, Autonomous Weapon Systems should be embedded within layered oversight mechanisms that priorities human agency and responsibility[3]. As military organizations continue to integrate Autonomous Weapons Systems into their intelligence and targeting processes, debates about verification standards, legal responsibility, and the humanitarian consequences of algorithmically mediated warfare are likely to remain central to the evolving governance of military artificial intelligence[4].

But the evidence and reports from the Swords of Iron indicate that algorithmic mediation improves the capabilities of the military, that it is an incremental change to the knowledge base that informs contemporary targeting decisions, and that it shows how commanders conceptually process information, understand what a 'target' is, and what constitutes lawful targeting. As individuals are increasingly labeled targets through probabilistic algorithmic classifications, the interpretive frame through which analysts and commanders understand them shifts. This captures the central claim of this study that AI-assisted warfare introduces a structural tension between computational efficiency and humanitarian restraint. In such environments, the challenge is no longer limited to keeping humans in the loop, but to ensure that human judgment remains meaningful. The study's normative arguments rely on an empirical basis; the processes described in this section - probabilistic classification at scale, compression of human review, institutionalized error tolerance, and the clinical consequences of these processes – are those of harming civilians, which was a feature of the observed targeting architecture that was structurally incompatible with IHL compliance

Digital Dehumanization and Accountability Gaps in AI-Assisted Warfare

This study offers a Gaza-focused analysis of AI-assisted warfare, reframing current developments as the opening phase of a new frontier. The systems under study are integral parts of a targeting infrastructure that accelerates the tempo of warfare while reducing

[1] Yuval Abraham, *Op. cit.* p. 2; The Guardian, *Israel's Use of AI in Gaza*, 2024, 'The machine did it coldly': Israel used AI to identify 37,000 Hamas targets | Israel-Gaza war | The Guardian (11.02.2026)

[2] United Nations Office for Disarmament Affairs, *Report of the 2023 Session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems – Advance Version*, CCW/GGE.1/2023/2, Geneva, 2023; United Nations General Assembly, *Lethal Autonomous Weapons Systems: Draft Resolution*, A/C.1/78/L.56, 2023

[3] Ilse Verdiesen, Filippo Santoni de Sio, Virginia Dignum, *Accountability and Control over Autonomous Weapon Systems: A Framework for Comprehensive Human Oversight*, "Minds and Machines", No. 31, 2021, pp.137–163 Avi Goldfarb and Jon Lindsay, *Artificial Intelligence in War: Human Judgment as an Organizational Strength and a Strategic Liability,* Brookings Institution, November 2020, p. 1, https://brookings.edu/research/artificial-intelligence-in-war/ (11.02.2026)

[4] Paul Scharre, *Op. cit.*, p. 531, p. 565; United Nations Office for Disarmament Affairs, *Report of the Group of Governmental Experts on Lethal Autonomous Weapons Systems*, 2023

complex social realities to simplified administrative categories.[1] The limited understanding of how their algorithmic outputs are generated creates a technical opacity gap. The flawed data environment in which they operated introduced and propagated systematic bias, reduced predictive validity, and produced unreliable outcomes. Their scaling effects significantly altered the operational workflow, creating an attribution. Strikes resulted in disproportionate civilian casualties compared to the anticipated military advantage, raising concerns about abuse of force and a breach of IHL. Beyond battlefield efficiency, these systems may have been deployed to signal military sophistication while testing and refining them under real conflict conditions. Taken together, this assemblage creates a "war-algorithm" environment where harm cannot be easily traced to a single decision-maker.[2] Against this backdrop, the study advances the normative position that responsibility for targeting decisions must reside with human operators, irrespective of the level of automation, as human agency is not removed but reconfigured through technological mediation[3].

Digital dehumanization refers to the "process where humans are reduced to data, which is then used to make decisions and/or take actions that negatively affect their lives"[4]. It is not a separate violation under international humanitarian law (IHL). Rather, it reshapes how existing legal obligations are carried out by shifting decision-making from contextual human judgment to probabilistic and data-driven assessments. In doing so, it can increase the likelihood that established IHL obligations, such as the prohibitions against indiscriminate or disproportionate attacks and the duty to take feasible precautions, are not meaningfully fulfilled[5]. In practice, this means that individuals may increasingly be evaluated through algorithmic patterns, metadata, or predictive indicators rather than through careful human assessment of their status and surrounding circumstances. In this sense, digital dehumanization operates similarly to automation bias: it is not itself an independent legal breach, but a condition that can make violations more likely. Its legal significance, therefore, lies in how it affects compliance with existing IHL obligations, particularly the duty of commanders to take all feasible precautions and to do everything feasible to verify that targets are lawful military objectives under Articles 57 and 58 of Additional Protocol I. Stauffer argues that autonomous systems can reduce human beings to mere data points, thereby instrumentalizing and dehumanizing those they target. However, this does not create new legal prohibitions under international humanitarian law (IHL). Instead, it raises concerns about how existing rules, particularly those relating to distinction, proportionality, and feasible precautions, are interpreted and applied in increasingly data-driven forms of warfare[6].

Algorithmic targeting becomes legally and ethically problematic when it relies on protected characteristics or treats civilian populations as undifferentiated data categories rather than individuals. While this does not automatically constitute a separate violation under international humanitarian law (IHL), it may undermine the principles of distinction,

---

[1] James C. Scott, *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*, Yale University Press, New Haven, 1998

[2] Dustin A. Lewis et al., *War-Algorithm Accountability*, Harvard Law School Program on International Law and Armed Conflict, 2016

[3] Ingvild Bode, Hendrik Huelss, *Autonomous Weapons Systems and Changing Norms in International Relations*, "Review of International Studies", Vol. 44, No. 3, 2018

[4] Soka Gakkai International, *Digital Dehumanisation Campaign*, 2025, p.1, https://sgi-peace.org/resources/digital-dehumanisation-campaign-videos (21.03.2026)

[5] Brian Stauffer, *A Hazard to Human Rights: Autonomous Weapons Systems and Digital Decision-Making*, Human Rights Watch, New York, 2025. https://www.hrw.org/report/2025/04/28/a-hazard-to-human-rights/autonomous-weapons-systems-and-digital-decision-making (21.03.2026)

[6] *Idem*

proportionality, and non-discrimination, and, in extreme cases, could raise concerns about collective punishment under Article 33 of the Fourth Geneva Convention[1].

Governing Algorithmic Warfare: Legal Responsibility and Policy Implications

As this analysis has shown, however, there were not only things that went wrong in Gaza, but also reasons why it was likely to go wrong, and it has shifted the question of accountability in Gaza from post-hoc analysis to prospective, structural regulation. This section opens with a methodological observation: the system under study is classified. This analysis thus relies on credible secondary sources rather than primary military documents. This limitation is not specific to this study but is inherent to the subject matter itself. The opacity of military AI systems is a core attribute of how states conduct their intelligence activities. What is analytically relevant is that data cannot be accessed through the structure. It is almost impossible for an external party to verify independently whether IHL is being complied with. In the military field, this epistemic gap is one of the main governance failures of algorithmic warfare, not because of a lack of lawfulness on the part of the military, but because there are no conditions for independent scrutiny[2]. This study is not intended to solve that problem; instead, it is working with that problem. Interpretative-analytical contributions are achieved by rigorously engaging with available data to yield defensible policy conclusions. The report on Autonomous weapons systems submitted to the UNGA by the Secretary-General in August 2024, which combined inputs from 73 states and 33 civil society organizations, made it clear that there is widespread concern that (AWS) systems have the potential to change warfare significantly and may strain, or even erode, existing legal frameworks[3]. The document was prepared without relying on classified Israeli military data. Yet, it reached conclusions on the application of IHL that were consistent with those developed in this study, indicating that the analytical approach is correct, even with a limited empirical basis

The need to ensure meaningful human control over the use of force has been highlighted by organizations such as the International Committee of the Red Cross and UN-based forums, particularly the Group of Governmental Experts on Lethal Autonomous Weapons Systems. This study contributes to this debate by deploying a case study to show how AI-assisted targeting systems may subtly erode such control in practice, by significantly altering the conditions under which human operators make decisions, rather than bypassing them outright.[4] By identifying specific gaps and associating them with processes of digital dehumanization, the study offers a pathway for attributing liability in contexts where targets are selected through flawed probabilistic classification, aligning with broader concerns that increasing automation may dilute, rather than eliminate, human judgment in the use of force.[5] It is pertinent to act on these observations rather than rely on the vacuous rhetoric of the

[1] Muzen Ismailovic, *Algorithmic targeting: the role of artificial intelligence in Israeli strikes in Gaza and its ethical implication*, "Éclairage", May 2025, https://www.grip.org/wp-content/uploads/2025/04/EC-2025-02-05-25-MI-IA-Israel-Gaza-version-finale-EN.pdf (21.03.2026)

[2] Vincent Boulanin, Dustin Lewis, *Responsible reliance concerning development and use of AI in the military domain*, "Ethics and Information Technology", Vol. 25, No, 1, 2023, pp. 1-15, https://doi.org/10.1007/s10676-023-09695-2

[3] United Nations Secretary-General. *Autonomous weapons systems: Report of the Secretary-General* (A/79/318). United Nations, 2024, pp. 1-77, https://documents.un.org/doc/undoc/gen/n24/238/45/pdf/n2423845.pdf (21.03.2026)

[4] International Committee of the Red Cross, *Autonomous Weapon Systems: Technical, Military, Legal and Humanitarian Aspects* (2019); United Nations Office for Disarmament Affairs, *CCW GGE LAWS Reports*, 2023

[5] Paul Scharre, *Op. cit.*, p. 277, p. 324

meaningful human control concept in governance. Normatively, of course, it is essential. Still, it has been given definitional inflation, with someone who reads a targeting recommendation for 20 seconds qualifying as doing an independent check, while someone who studies it, reads it twice, considers their own options, and secures agreement from others does not. The following mechanisms offer a more precise regulatory agenda.

Mandatory Algorithmic Auditability Standards*:* Pre-deployment and ongoing auditability requirements should apply to any targeting system used during armed conflict that AI assists. The decision-making logic in the system, including training data, weighting rules, error margins, and output thresholds, must be interpretable and documented by a qualified and independent auditor. This is not only possible but has been done in civilian AI regulation: the European Union's Artificial Intelligence Act requires high-risk AI systems to maintain comprehensive technical documentation and to provide opportunities for human oversight throughout the system's lifecycle. If the same standard were applied to military AI, a state using AI would have to keep logs of the algorithm sufficient to allow post-incident compliance with IHL to be reviewed. Meanwhile, language on traceability and explainability has been added to the rolling text of the CCW Group of Governmental Experts for November 2024, in which auditability is beginning to secure a foothold in multilateral discussions.[1] This study supports this approach and suggests that this should be strengthened to a legally binding commitment in any future binding document.

Disaggregated Liability Attribution Frameworks: There are two aspects to the accountability gap: doctrinal and institutional. Under the current command responsibility doctrine, a superior is held liable for crimes committed by subordinates if the superior knew or should have known of the crime and failed to prevent or punish the perpetrators, as stipulated in Article 28 of the Rome Statute. The issue with algorithmic targeting is that there are several actors between the data, the algorithm's training, its deployment, and the civilian harm it causes. For this entire chain, Bo et al. have suggested a framework for traceability based on responsibility for IHL throughout the chain, not just at the end, where the final strike is delivered[2]. This study supports this and urges its incorporation into domestic military law, as well as into the draft of a legally binding instrument on Lethal Autonomous Weapons Systems (LAWS). Specifically, there should be a requirement for states to prepare a liability attribution map documenting who is responsible for each decision node in the algorithmic targeting cycle before it is deployed.

Minimum Verification Time and Human Oversight Protocols: Perhaps the most tractable reform is the procedural conditions of human review. The documented 20-second review windows and the gender-confirmation verification task, which is usually the primary verification task, constitute a de facto displacement of the precautionary duty, even when humans nominally are in the loop. There should be a minimum number of steps in the process of reviewing AI-generated target recommendations, such as a minimum review time, independent verification of the data used to generate the target, consultation with legal advisors if the AI is likely to result in significant civilian casualties, mandatory documentation of the proportionality assessment undertaken, and so on. This is a way to operationalize the Convention on Certain Conventional Weapons (CCW) rolling text's context-appropriate

[1] Benjamin Perrin, *Lethal Autonomous Weapons Systems & International Law: Growing Momentum Towards a New International Treaty*, "Insights", Vol. 29, No. 1, 2025, pp. 1-8, https://asil.org/wp-content/uploads/2025/10/ASIL_Insights_2025_V29_I1.pdf (21.03.2026)

[2] Marta Bo, Laura Bruun, Vincent Boulanin, *Retaining Human Responsibility in the Development and Use of Autonomous Weapon Systems: On Accountability for Violations of International Humanitarian Law Involving AWS*, "Stockholm International Peace Research Institute", 2022. https://doi.org/10.55163/AHBC1664

human oversight, particularly in morally and legally significant decisions, such as identification and/or engagement of targets. [1] It is also directly responsive to the mechanistic and compressed review process, identified as a key structural weakness in Gaza, which is the focus of this study.

All three mechanisms are individually insufficient. They complement each other and are essential elements of a governance structure appropriate to algorithmic warfare. Their incorporation into a legally binding document, which now has significant international momentum after a UNGA resolution on 62nd Dec 2024 passed by a UN vote of 166 countries[2], is the least regulatory response that Gaza's experience demands.

Rethinking IHL in AI-Mediated Conflict

The application of the principles of distinction, proportionality, and precaution is increasingly mediated by systems that priorities scale, speed, and pattern recognition, highlighting a widening gap between international humanitarian law and the operational realities of AI-assisted warfare. In such environments, digital dehumanization emerges as an operational by-product of processes that reduce individuals to probabilistic profiles. As Scharre observed, the growing reliance on machine-generated outputs can tilt human judgment toward system recommendations, subtly recalibrating perceptions of acceptable risk in the use of force.[3] When combined with large-scale data processing and compressed decision timelines, this shift raises the possibility that legal protections for civilians may be progressively eroded in practice, even if they remain intact in principle. The inadequacy of existing IHL frameworks in the context of AI-assisted targeting is demonstrable through a close reading of how each of the three cardinal principles operates under conditions of algorithmic mediation.

The Principle of Distinction: Customary IHL and Article 48 of Additional Protocol I require that parties to an armed conflict distinguish at all times between civilians and combatants, as well as between civilian objects and military objectives. This obligation implies that a person's status is to be determined individually and in context when making decisions about attacks. What the Gaza case reveals is that targeting systems based on algorithms failed to replace individualized assessment with probabilistic approximations based on behavioral proxies such as shared communication metadata, social network connections, and digital infrastructure. This is not only a legal issue of the unreliability of such a proxy, but it was also evident that it was. It is because IHL's distinction obligation is, by design, a qualitative judgment that assumes human ability to make contextual inferences, something a machine learning model trained on aggregate data patterns is not able to do. In situations of asymmetric warfare in urban areas, protected civilian status is something that can only be judged by human assessment, which is often contextual and intuitive, and is not a field that algorithms excel at. [4] The sheer scale of Lavender's classification exercise, which designated some 37,000 people as suspected militants within weeks, is a sign of the move away from individual judgment that is required[5]. Such a volume of a model is required to be

[1] Benjamin Perrin, *Op. cit.*, p. 5
[2] Human Rights Watch, *Killer Robots: UN Vote Should Spur Treaty Negotiations,* HRW, New York, 2024, pp. 1-3, https://www.hrw.org/news/2024/12/05/killer-robots-un-vote-should-spur-treaty-negotiations (21.03.2026)
[3] Paul Scharre, *Op. cit.*, p. 98, 146, p. 279
4 International Committee of the Red Cross, *Autonomous weapon systems and international humanitarian law,* March 2026, https://www.icrc.org/sites/default/files/2026-03/4896_002_Autonomous_Weapons_Systems_-_IHL-ICRC.pdf (21.03.2026)
[5] Yuval Abraham, *Op. cit.*, p. 3

pattern-matching, and not assessing. Thus, it is a mismatch between the technology and what IHL needs.

The Principle of Proportionality*:* The proportionality rule, codified in Additional Protocol I - Article 51(5)(b), stipulates that attacks that are likely to cause civilian injury that is excessive in relation to the specific and direct military advantage to be gained are prohibited. The assessment is very much prospective and comparative: weighing incommensurable values - expected civilian casualties versus expected military gains - to make a decision. This includes a type of thinking that combines legal, military, and moral reasoning in real time. [1] This is not the kind of reasoning performed by an AI-assisted targeting system. They make recommendations based on pattern recognition and risk thresholds. Reported collateral damage limits, allowing up to 15 civilian casualties for top Hamas officials, and fewer for lower-ranking members of the organization[2], were not the result of the use of true proportionality analysis in the Gaza context. They were predefined parameters programmed into the algorithms, which were then used to operationalize them at scale. The legal impact is important because a pre-formulated collateral threshold, imposed in the same manner against all algorithmically generated targets, is not a proportionality exercise but an alternative to one. The human command decision-making process under IHL has already been replaced by an algorithm that determines acceptable casualty ratios before any human commander is consulted[3].

The Principle of Precaution: In accordance with Articles 57 and 58 of Additional Protocol I, parties must take all practicable measures to ensure that the target of an attack is a legitimate military objective, to select means and methods which minimize incidental civilian injury and damage, and to cease or suspend an attack if it becomes evident that it will cause civilian suffering that is clearly disproportionate to the direct military advantage[4]. The duty of precaution is thus the duty of active inquiry, as commanders must ask whether their intelligence is valid and whether their targets are legitimate and therefore worthy of attack. The 20-second period in Gaza operations, during which all names were documented, and the delegation of gender confirmation as the main verification task[5], are not consistent with any sensible interpretation of the precautionary obligation. The doctrine of an accepted error margin in the classification of algorithms is the reverse of the error as a trigger for further examination.

These observations, when taken together, help to make sense of the claim of structural inadequacy. The issue isn't that IHL principles aren't applicable; distinction, proportionality, and precaution apply to everyone, including those using artificial intelligence systems. The structural issue is the conditions under which algorithmic targeting is employed, such as the statistical classification of large populations, tight decision timelines, institutionalized error tolerances, and automation biases, all of which undermine the cognitive and institutional practices needed to uphold these principles meaningfully. Bruun et al. acknowledge that IHL compliance should not ignore the human element of the conduct-of-hostilities rules, which

[1] Laura Bruun, Marta Bo, Netta Goussac, *Compliance with international humanitarian law in the development and use of autonomous weapon*, "Stockholm International Peace Research Institute", 2023, https://www.sipri.org/sites/default/files/2023-03/ihl_and_aws.pdf (21.03.2026)
[2] Yuval Abraham, *Op. cit.*, p. 2
[3] Gerald Mako, *Legal accountability for AI-driven autonomous weapons*, March 9, 2026, https://lieber.westpoint.edu/legal-accountability-ai-driven-autonomous-weapons/ (21.03.2026)
[4] Laura Bruun, Marta Bo, Netta Goussac, *Op cit*., p. 28
[5] Yuval Abraham, *Op. cit.*, p. 3.

remain the foundation for IHL[1]. The Gaza experience shows just the opposite: the operational structure of targeting with the help of AI did the opposite. For this reason, the governance of military artificial intelligence must rest on a reaffirmation of meaningful human control. Legal frameworks must tighten oversight standards, verification, and attribution. Without such reforms, the integration of AI into targeting processes risks entrenching a model of warfare in which technological capability outpaces law's capacity to regulate its consequences.

Bibliography

Books

1. Arkin, Ronald C., *Governing Lethal Behavior in Autonomous Robots*, CRC Press, Boca Raton, 2009
2. Barocas, Solon; Hardt, Moritz; Narayanan, Arvind, *Fairness and Machine Learning*, MIT Press, 2023
3. Bruun, Laura; Bo, Marta; Goussac, Netta, *Compliance with International Humanitarian Law in the Development and Use of Autonomous Weapons*, Stockholm International Peace Research Institute, 2023
4. Chamayou, Grégoire, *A Theory of the Drone*, trans. Janet Lloyd, The New Press, New York, 2015
5. Crawford, Kate, *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*, Yale University Press, New Haven, 2021
6. Gillespie, Tarleton, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*, Yale University Press, New Haven, 2018
7. Horowitz, Michael C., *The Diffusion of Military Power: Causes and Consequences for International Politics*, Princeton University Press, Princeton, 2010
8. Latour, Bruno, *Reassembling the Social: An Introduction to Actor-Network-Theory*, Oxford University Press, Oxford, 2005
9. Lewis, Dustin A. et al., *War-Algorithm Accountability*, Harvard Law School Program on International Law and Armed Conflict, 2016
10. O'Neil, Cathy, Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy, Crown *Publishing*, New York, 2016
11. Scharre, Paul, *Army of None: Autonomous Weapons and the Future of War*, W. W. Norton & Company, New York, 2018
12. Scott, James C., Seeing *Like a State: How Certain Schemes to Improve the Human Condition Have Failed*, Yale University Press, New Haven, 1998
13. Suchman, Lucy, *Human-Machine Reconfigurations: Plans and Situated Actions*, 2nd Ed., Cambridge University Press, Cambridge, 2007

Studies and Articles

1. Abraham, Yuval, *A Mass Assassination Factory: Inside Israel's Calculated Bombing of Gaza*, "+972 Magazine", November 30, 2023
2. Abraham, Yuval, *Lavender': The AI Machine Directing Israel's Bombing Spree in Gaza*, "+972 Magazine and Local Call", April 3, 2024
3. Abraham, Yuval, "Lavender: The AI Machine Identifying Targets in Israel's Gaza War", "+972 Magazine", April 2024
4. Anderson, Kenneth; Waxman, Matthew, *Law and Ethics for Autonomous Weapon Systems: Why a Ban Won't Work and How the Laws of War Can*, "Hoover Institution Working Paper on National Security, Technology, and Law", 2013

[1] *Idem*

5. Bo, Marta; Bruun, Laura; Boulanin, Vincent, *Retaining Human Responsibility in the Development and Use of Autonomous Weapon Systems: On Accountability for Violations of International Humanitarian Law Involving AWS*, Stockholm International Peace Research Institute, 2022
6. Boulanin, Vincent; Lewis, Dustin A., *Responsible Reliance Concerning Development and Use of AI in the Military Domain*, "Ethics and Information Technology", Vol. 25, No. 1, 2023
7. Homayounnejad, Maziar, *Regulating Lethal Autonomous Weapon Systems I: Assessing the Sense and Scope of 'Autonomy'*, in "Emerging Military Weapon Systems" TLI Think Paper 76/2017, The Dickson Poon School of Law, King's College London, 2017
8. Ismailovic, Muzen, *Algorithmic Targeting: The Role of Artificial Intelligence in Israeli Strikes in Gaza and Its Ethical Implications*, "Éclairage", May 2025
9. Kalluri, Pratyusha, *Don't Ask If Artificial Intelligence Is Good or Fair, Ask How It Shifts Power*, "Nature", Vol. 583, 2020
10. Mako, Gerald, *Legal Accountability for AI-Driven Autonomous Weapons*, Lieber Institute for Law & Warfare, March 9, 2026
11. Maroonian, Anaïs, *Proportionality in International Humanitarian Law: A Principle and a Rule*, Lieber Institute for Law and Warfare, October 2022, https://lieber.westpoint.edu/proportionality-international-humanitarian-law-principle-rule/
12. McKernan, Bethan; Kierszenbaum, Quique, *Israel's Use of AI in Gaza Targeting Raises Questions over Civilian Harm*,"The Guardian", April 5, 2024
13. Parasuraman, Raja; Riley, Victor, *Humans and Automation: Use, Misuse, Disuse, Abuse*, "Human Factors", Vol. 39, No. 2, 1997
14. Perrin, Benjamin, *Lethal Autonomous Weapon Systems & International Law: Growing Momentum Towards a New International Treaty*, "ASIL Insights", Vol. 29, No. 1, 2025
15. Roff, Heather M., *The Strategic Robot Problem: Lethal Autonomous Weapons in War*, "Journal of Military Ethics", Vol. 13, No. 3, 2014
16. Schmitt, Michael N., *Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics*, Harvard National Security Journal Feature, 2013
17. Sharkey, Noel, *The Evitability of Autonomous Robot Warfare*, "International Review of the Red Cross", Vol. 94, No. 886, 2012
18. Stauffer, Brian, *A Hazard to Human Rights: Autonomous Weapons Systems and Digital Decision-Making,* Human Rights Watch, New York, 2025
19. Verdiesen, Ilse; Santoni de Sio, Filippo; Dignum, Virginia, *Accountability and Control over Autonomous Weapon Systems: A Framework for Comprehensive Human Oversight*," Minds and Machines, Vol. 31, 2021
20. Winter, Elliot, *The Compatibility of Autonomous Weapons with the Principles of International Humanitarian Law*, Journal of Conflict and Security Law, Vol. 27, No. 1, 2022
21. Wiese, Lisa; Langer, Charlotte, *Gaza, Artificial Intelligence, and Kill Lists*, Verfassungsblog, May 16, 2024

Documents

1. Diakonia, *Basic Principles of International Humanitarian Law*, Diakonia, https://www.diakonia.se/ihl/resources/international-humanitarian-law/basic-principles-ihl/
2. International Committee of the Red Cross, *Autonomous Weapon Systems and International Humanitarian Law*, 2026
3. International Committee of the Red Cross, *Autonomous Weapon Systems: Implications of Increasing Autonomy in the Critical Functions of Weapons*, ICRC, Geneva, 2016
4. International Committee of the Red Cross, *Autonomous Weapon Systems: Technical, Military, Legal and Humanitarian Aspects*, 2019
5. United Nations Secretary-General, *Autonomous Weapons Systems: Report of the Secretary-General,* (A/79/318), United Nations, 2024

6. Stockholm International Peace Research Institute, *Autonomy in Weapon Systems and the Military Applications of Artificial Intelligence*, SIPRI, Stockholm, 2024
7. International Committee of the Red Cross, *Customary International Humanitarian Law, Volume I: Rules*, Cambridge University Press, Cambridge, 2005
8. Soka Gakkai International, *Digital Dehumanisation Campaign*, 2025
9. US Department of Defense, *Directive 3000.09: Autonomy in Weapon Systems*, DoD, Washington, D.C., Updated 2023, Sec. 3(a)
10. Human Rights Watch, *Killer Robots: UN Vote Should Spur Treaty Negotiations*, Human Rights Watch, New York, 2024
11. United Nations General Assembly, *Lethal Autonomous Weapons Systems: Draft Resolution*, A/C.1/78/L.56, 2023
12. Human Rights Watch, *Losing Humanity: The Case Against Killer Robots*, Human Rights Watch, New York, 2012
13. United Nations, *Report of the 2019 Session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems*, CCW/GGE.1/2019/3, United Nations Office, Geneva, 2019
14. United Nations Office for Disarmament Affairs, *Report of the 2023 Session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems*, CCW/GGE.1/2023/2, Geneva, 2023
15. United Nations Office for Disarmament Affairs, *Report of the Group of Governmental Experts on Lethal Autonomous Weapons Systems*, 2023
16. United Nations Institute for Disarmament Research, *The Weaponization of Increasingly Autonomous Technologies: Autonomous Weapon Systems and Cyber Operations*, UNIDIR, Geneva, 2017

Websites

1. https://ssrn.com/
2. https://verfassungsblog.de/
3. https://www.972mag.com/
4. https://www.amnesty.org/
5. https://www.businessinsider.com/
6. https://www.hrw.org/
7. https://www.icrc.org/
8. https://www.lemonde.fr/
9. https://www.rusi.org/
10. https://www.sipri.org/
11. https://www.theguardian.com/